REMARKS

Reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks is respectfully requested. Entry of this Amendment under Rule 116 is merited as it raises no new issues and requires no further search.

Claims 1-12, 14-23 and 26 are pending in the application. Claims 1, 21 and 23 have been amended to improve claim language. Claims 24-25 have been cancelled without prejudice or disclaimer to simplify the issues. No new matter has been introduced through the foregoing amendments.

The Examiner's objection to claim 1 as manifested in paragraph 3 of the Final Office Action is noted. The wording being objected to has been amended to overcome this objection and to be consistent with line 5 of claim 1, i.e., at least one correlator.

The Examiner's objection to claims 1, 23-26 as manifested in paragraph 4 of the Final Office Action is believed overcome, because claims 1 and 23 have been amended in the manner kindly suggested by the Examiner.

The Examiner's 35 U.S.C. 112, second paragraph rejection of claim 1 as manifested in paragraph 6 of the Final Office Action is traversed, because contrary to the Examiner's assertion, the wording "event driven correlation services" does not lack antecedent basis.

The Examiner's 35 U.S.C. 112, second paragraph rejections of claims 21 and 23 as manifested in paragraphs 6-7 of the Final Office Action are believed overcome, because claims 21 and 23 have been amended in the manner kindly suggested by the Examiner. The amended wording "said event driven correlation" of claim 23 has antecedent basis in the amended wording "an event driven correlation" of claim 21 from which claim 23 depends.

The Examiner's statement in paragraph 8 of the Final Office Action that "Applicant is agreeing with the prior art disclosure" is inaccurate and, therefore, traversed. Nowhere in the Amendment filed April 13, 2005, did Applicants state that they are agreeing with the prior art disclosure. Applicants simply pointed out that Moran is distinguishable from the claimed invention in that it teaches a data driven mechanism. *See* the April 13, 2005 Amendment, page 7, lines 4-5

from bottom.

The Examiner's statement in paragraph 9 of the Final Office Action is noted. Applicants respectfully disagree with the Examiner because Moran, as briefly discussed in the paragraph bridging pages 4-5 of the Final Office Action, clearly fails to teach or suggest the presently claimed event driven correlation.

The Examiner's argument in paragraph 10 of the Final Office Action is further noted. Applicants respectfully disagree with the Examiner because Moran, as briefly discussed in the last full paragraph on page 5 of the Final Office Action, clearly fails to teach or suggest the presently claimed event driven correlation. A detailed explanation will be provided herein below with respect to the Examiner's repeated art rejections.

The Examiner's statement in paragraph 11 of the Final Office Action that "Applicant clearly has failed to explicitly identify specific claim limitations which would define a patentable distinction over prior arts" is inaccurate and, therefore, traversed. In the Amendment filed April 13, 2005, Applicants have explicitly identified a specific claim limitation, i.e., event driven correlation, which defines a patentable distinction over the applied prior art. *See* the April 13, 2005 Amendment, page 7, lines 4-5 from bottom.

The 35 U.S.C. 102(e) rejection of claims 1-12 and 14-26 as being anticipated by Moran is traversed for the reason advanced in the April 13, 2005 Amendment which is incorporated by reference herein. The anticipatory rejection relying on Moran is also flawed for the further reasons presented below.

1. Moran clearly fails to teach or disclose the limitation "at least one data gathering component which gathers kernel audit data **and** syslog data" recited in independent claim 1. In other words, claim 1 requires that the data gathering component gather both kernel audit data and syslog data. Applicants respectfully submit that Moran fails to teach or disclose a data gathering component that gathers **kernel audit data**.

The Examiner's reliance on column 8, lines 6-46 and column 10, lines 14-49 of Moran for the claim limitation at issue is noted. However, the cited passages of Moran fail to include an enabling disclosure of the claimed data gathering component that gathers kernel audit data. The

cited passages are reproduced below for the Examiner's convenience of review.

In particular, Moran teaches in column 8, lines 6-23 the following:

> "The architecture of an embodiment of the inventive intrusion detection system is shown in FIG. 3. A user interface 300 on a console (FIG. 4 shows an exemplary display on the user interface 300) provides the system administrator with access to the analysis engine 302 and event database 304. Analysis engine 302 utilizes ruleset 306 and an attack signatures database 308, and receives input from sensor controller 310. The sensor controller 310 is in communication with various sensors (in the form of data collection modules) 312, and may pass information to the event database 304. For efficiency and ease of use, the sensor controller 310 may be combined with the sensors 312 into a single program or process, as shown by dotted box 314, but the sensors 312 may individually or collectively be run independently of the sensor controller 310. Although the architecture has been presented in terms of a specific embodiment, one skilled in the art will recognize that the various elements shown may be combined in different ways, or further separated into other elements."

This paragraph discloses how the sensors, which are believed to be considered by the Examiner to read on the claimed data gathering component, in FIG. 3 of Moran are arranged and connected to other components of the Moran system. However, the paragraph does not teach or disclose whether the sensors gather kernel audit data or not.

Moran teaches in column 8, lines 24-35 the following:

> "The inventive system may be used in conjunction with a larger real-time, network-based intrusion detection system (IDS), such as that described in co-pending U.S. patent application Ser. No. 09/615,967. In this configuration, the inventive system uses the network-based IDS as one of its sensors, and can be triggered to investigate further upon receiving a signal from the network-based IDS about suspicious events from other platforms (hosts, routers, and network monitors). The inventive system can be used to evaluate suspicious events in a larger context, and provide a response that the IDS uses in scoring the event to determine whether to issue an alert, and what level to assign it."

This paragraph discloses that the system of Moran can be used in a network-based IDS. However, the paragraph does not contain any disclosure of a data gathering component and is, therefore, believed irrelevant to the claim limitation at issue.

Moran teaches in column 8, lines 36-46 the following:

"By combining the inventive system with the real-time IDS, the high false positive rate typical of the real-time systems is reduced by filtering out false alerts using a broader range of information than the IDS can retain, and by allowing the alert threshold to be set higher, because the inventive system can recover information about a suspicious session that occurred before the threshold was crossed. Further, in conjunction with the inventive system, the real-time IDS can monitor higher traffic rates, because it can now ignore certain classes of events that will be recovered by the inventive system."

This paragraph discloses advantages that the system of Moran can provide if it is used in a real-time IDS. However, the paragraph does not contain any disclosure of a data gathering component and is, therefore, believed irrelevant to the claim limitation at issue.

Moran teaches in column 10, lines 14-32 the following"

"The inventive system comprises data collection modules and an analysis engine. Preferably, the data collection modules are separate programs, allowing them to run on the compromised computer and optionally send the extracted information to another (hopefully uncompromised) computer for analysis. The data collection modules are designed to be lightweight and relatively simple, and different data sources are handled by different modules. These modules extract the data and add identifying information for the fields, simplifying the task for the analysis engine, which may have to deal with variants of the information from different platforms. Keeping the data collection modules lightweight and simple also simplifies the task of porting them to new platforms with differences in the data available and its format. This segmentation of functionality also makes it easy to extend the system, allowing both the addition of new data sources and the addition of rules on what evidence to collect and how to combine and interpret it."

This paragraph discloses several reasons why the data collection modules, which are believed to be considered by the Examiner to read on the claimed data gathering component, should be made simple and lightweight. The most relevant teaching includes "[t]hese modules extract the data and add identifying information for the fields," at column 10, lines 21-22. However, the paragraph as a whole and the above mentioned most relevant teaching in particular clearly fail to teach or disclose that the data collection modules gather kernel audit data.

Finally, Moran teaches in column 10, lines 33-49 the following:

"The DERBI system referenced above looks for evidence of exploits, and the evidence of other components of attacks is limited to what can be collected by traditional configuration checkers. The system of the invention is able to utilize such evidence and data sources used by system administrators and others investigating

> and tracking attackers, in addition to additional data sources collected by the data collection modules. Some of these data sources have been examined using tools provided as part of the operating system, some have been examined using custom tools, and some are handled by scripts and ad hoc programs that never became widely available. Such tools are intended to reduce the level of effort needed to deal with individual data sources, by taking information collected for system administration and customizing it for various computer tasks. They extract data from system logs and other files, filter it, and display it to the system administrator."

This paragraph discusses that the Moran system is able to process other data sources which are not colleted by the data collection modules. The other data sources include system logs, which appear to be read by the Examiner on one of the data types that the claimed data gathering component gathers, but do not include kernel audit data which is the other data type that the claimed data gathering component collects.

Accordingly, Applicants respectfully submit that Moran as applied by the Examiner fails to teach or disclose the claimed data gathering component that gathers kernel audit data.

2. Moran clearly fails to teach or disclose the limitation "said at least one correlator uses **event driven** correlation services having an ECS (Event Correlation Services) engine core" recited in independent claim 1.

During examination, the claims must be interpreted as broadly as their terms reasonably allow. In re American Academy of Science Tech Center, 2004 WL 1067528 (Fed. Cir. May 13, 2004). This means that the words of the claim must be given their plain meaning **unless applicant has provided a clear definition in the specification**. In re Zletz, 893 F.2d 319, 321, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989); Chef America, Inc. v. Lamb-Weston, Inc., 358 F.3d 1371, 1372, 69 USPQ2d 1857 (Fed. Cir. 2004). See also MPEP, section 2111.01.

The term "event driven" has been given a clear definition in the specification, at page 24, lines 1-4, under the heading "ECS Terminology" at page 22, line 26. Specifically, the tern "event driven" means that events arriving, e.g., at the engine core, trigger processing. Applicants respectfully submit that Moran does not teach or disclose the claimed event driven correlation services.

The Examiner's reliance on column 4, lines 25-36 and column 11, lines 15-54 of Moran for

the claim limitation at issue is noted. However, the cited passages of Moran fail to include an enabling disclosure of the claimed event driven correlation services. The cited passages are reproduced below for the Examiner's convenience of review.

In particular, Moran teaches in column 4, lines 25-36 the following:

> "In another embodiment, an intrusion detection system comprises a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file, filter out expected time steps, correlate them with other events, and assign a suspicion value to a record associated with an event. In a further embodiment, the system compares the timestamps of a directory and its files and identifies values that are inconsistent or not accounted for, and assigns a suspicion value to the associated file or directory. In a further embodiment, directory and file timestamps from archival sources (e.g., backup tapes) are used to extend the data used in the assessment of the current state of the filesystem."

This paragraph discloses how timestamps are processed by a mechanism of the Moran system. However, the paragraph does not disclose whether the mechanism's processing is triggered by the arrival of events in the presently claimed manner or not.

Moran teaches in column 11, lines 15-27 the following:

> "In an embodiment of the invention, the primary data source is the computer's filesystem, and multiple correlations are checked between files. Changes to system files and directories is a key component of many intrusions. Since system directories change infrequently and in largely predictable ways, attacks often leave a system directory in a state that is not only inconsistent with normal practice, but that is indicative of a particular class of attacks. This evidence is obtained by correlations between dates on the files and the directory, between dates on files and their relative order in the directory, and on dates of files relative to the information left in a directory when a file is deleted or removed."

This paragraph discloses that file systems and system files can provide evidence of intrusions. This teaching is completely irrelevant to the claim limitation at issue, i.e., whether processing is triggered by events' arrival or not.

Moran teaches in column 11, lines 28-40 the following:

> "The inventive system may also search the filesystem, including deleted entries, for filenames and filename patterns that are known parts of attacks, such as names that are part of attack scripts in circulation or use, and names that are part of the standard operating practice/modus operandi of attackers. Filesystem information,

> both timestamps and file signatures, may be recovered from backup dumps without having to reload the files and directories to disk. In an embodiment of the invention, the system supports the ufsdump format, which is the most commonly used on a range of UNIX systems, and supports additional dump formats with data collection modules as needed."

This paragraph further details how file systems and system files can provide evidence of intrusions. This teaching is completely irrelevant to the claim limitation at issue, i.e., whether processing is triggered by events' arrival or not.

Finally, Moran teaches in column 11, lines 41-54 the following:

> "Some of the programs most likely to be involved in an attack produce log entries for significant events. Some of these put related, often overlapping, information into different log files. There are commonly available hacker tools that help an attacker hide his tracks by deleting selected entries from these files, but these tools leave evidence of the deletion behind. Thus, the inventive system scans log files looking for evidence of an attack and for inconsistencies between the following:
> entries within each log file,
> related entries in different log files, and
> entries in the log file and information that is expected to be found within the filesystem (for example, between a user's login entries and his login start up files)."

This paragraph is also irrelevant because it only discusses how log files are processed, whereas the main issue is whether the log file processing is triggered upon events' arrival.

Accordingly, Applicants respectfully submit that Moran as applied by the Examiner fails to teach or disclose the claimed event driven correlation.

The anticipatory rejection of independent claim 1 and its dependent claims is therefore erroneous and should be withdrawn.

3. As to independent claim 19, Applicants respectfully submit that the applied reference of Moran fails to teach or disclose at least the claimed "**reformatting means** for reformatting each of the read kernel records into a different format."

The Examiner's reliance on column 9, line 54 through column 10, line 32 of Moran for the claim limitation at issue is noted. However, the cited passage of Moran fails to include an enabling disclosure of the claimed reformatting means for reformatting each of the read kernel records into a different format. The cited passages are reproduced below for the Examiner's convenience of

review.

In particular, Moran teaches in column 9, lines 54-66 the following:

> "The system in accordance with the invention is preferably configured to assume that those additional data sources will not be present, but is able to utilize them if they are. The inventive system uses secondary and indirect information, and this expanded consideration of data sources occurs along two dimensions: (1) it uses multiple sources of data about the same event (although it is not unusual for there to be no usable information on an event, because it may not have been collected or it may have been deleted either maliciously or in normal course of operations); and (2) it identifies chains of events, inferring information about any potential "missing links." The pattern of a typical network-based attack is shown in FIG. 4."

This paragraph discloses additional information that the Moran system is configured to process. It does not disclose whether the additional information is reformatted into a different format or not. The paragraph is therefore irrelevant to the claim limitation at issue.

Moran teaches in column 9, line 67 through column 10, line 13 the following:

> "The inventive system has improved ability to catch attacks having novel components, because it is far less likely that all the components of the attack will be unknown to the system. For example, new exploits to gain root privilege are being discovered all the time, but the number of methods of installing and concealing a backdoor changes very slowly. Similarly, the methods for cleaning up log files and other evidence has changed very slowly over the years. Hacker "tradecraft" (modus operandi) produces atypical behaviors that are detected by the inventive system. For example, common tradecraft is to hide a directory by beginning its name with ".." (dot-dot) because it is not displayed in the normal listings of the parent directory. This and other patterns are easily identified by the system of the invention, as will be described herein."

This paragraph discloses the Moran system's ability to catch novel hacking attacks. It is completely irrelevant to the claim limitation at issue.

Finally, as discussed above, Moran teaches in column 10, lines 14-32 several reasons why the data collection modules should be made simple and lightweight. The most relevant teaching includes "[t]hese modules extract the data and add identifying information for the fields," at column 10, lines 21-22. However, "extract data" is completely different from "reformat [data] into a different format." Thus, the paragraph as a whole and the above mentioned most relevant teaching in particular clearly fail to teach or disclose the claimed reformatting means.

Accordingly, Applicants respectfully submit that Moran as applied by the Examiner fails to teach or disclose the claimed reformatting means of claim 19. The anticipatory rejection of independent claim 19 and its dependent claim 20 is therefore erroneous and should be withdrawn.

4. As to independent claim 21, the Moran reference clearly fails to teach or disclose the claimed **reformatting each of the read kernel records into a different format**, as argued above with respect to claim 19, and the claimed **event driven** correlation, as argued above with respect to claim 1. The anticipatory rejection of independent claim 21 and its dependent claims is therefore erroneous and should be withdrawn.

5. Should the Examiner insist that Moran teaches or discloses each and every element of the rejected claims, the Examiner is kindly asked to specify **with reasonable clarity** how the claim elements are taught by Moran. As discussed above, the current rejection cites, for each claim limitation, numerous, and mostly irrelevant, paragraphs. This makes it very difficult for Applicants to properly understand and respond to the rejection. The Examiner's cooperation is respectfully requested and would be greatly appreciated.

All claims in the present application are believed patentable over the art as applied by the Examiner. Early and favorable indication of allowance is courteously solicited.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,

LOWE HAUPTMAN & BERNER, LLP

Benjamin A. Hauptman
Registration No. 29,310

1700 Diagonal Road, Suite 300
Alexandria, VA 22314
(703) 684-1111
(703) 518-5499 Facsimile
Date: August 29, 2005